From: coats@ntrnet.net@inetgw
To: Microsoft ATR
Date: 1/23/02 11:49am
Subject: Microsoft Settlement

Dear Sirs:

It is my considered opinion as a mathematician and computer scientist of long standing (Ph.D., MIT: 1978) that the combination of Microsoft's software design practices and continued aggressively linking monopolies across software disciplines constitutes a serious risk both to the national security and to the economic interests of the United States as a whole.

Microsoft has aggressively pursued a strategy of tying across its entire product line. This is evident not only in its sales practices but also in the behavior of its upgrades: for example, it has been all but impossible for ordinary users to upgrade _any_ Microsoft product (whether
operating system or office software) without both installing Microsoft's "Outlook" email software and also overriding the user's installed email software with "Outlook".

This tying across product lines affects both the national economic interest ant the national security because of inherent vulnerabilities in Microsoft's software design practices. This past year has been a bad year for so-called "worms" and "viruses" damaging information systems and causing denial of service all over the Internet. Network consulting guru Jakob Nielsen (see http://www.useit.com/) estimates this past year's consequent economic damage as in excess of $170 Billion.
I have personally experienced two days of complete network outage due to serious Outlook-worm attacks to backbone provider Verozon (who have not admitted it publically; however, MCNC is responsible for backbone load analysis for the southeast, and the load-signature of these attacks is unmistakeable.)

More than 80% of those attacks are "Outlook" specific: they do not affect other email software (such as the previous market-leader "Eudora") at all. More than 98% of the attacks are Microsoft specific. The reason for these vulnerabilities is inherent in Microsoft's "active content" document design, where documents are no longer simply data to be processed or viewed, but are actually programs (written in "Visual Basic" with "ActiveX" controls) that can take over the user's computer and compromise it. This makes it easy for Microsoft to provide "glitz" but at the expense of using an approach which is inherently insecure. (Of the remaining 2% of network attacks, a large majority are due to other -- cross-platform -- "active content" attacks,

specifically employing JavaScript and Java!)

Hundreds of billions of dollars in consequent damages to the national information infrastructure mean that it is in the national interest to prevent this kind of cross-system tying. Furthermore, it is in the national security interest to ensure that Federal Interest Computers are not subject to the kinds of attacks that Microsoft has made possible. I think the following remedies are in order:

1. Microsoft must be made to stop the software-level tying between different kinds of software systems. Specifically, there should not be shared content between:
   (a) operating systems;
   (b) application software;
   (c) network server software.
   If achieving this means splitting the company along these lines into three separate entities, then so be it.

2. Microsoft software, with its vulnerable cross-system ties, should not be allowed on Federal Interest Computers. Arguably, it should not be allowed on any system networked to a Federal Interest Computer, but that latter is admittedly a rather drastic step.

3. Microsoft's "patches" and "upgrades" should be required to confine themselves to the ostensible purpose that they have; they should be forbidden to change other software systems on the user's computer without express notice and consent.

4. Microsoft's upgrade practices, in which the upgrade-system silently replaces the user's email software setup with "Outlook", has had that effect on current Federal Interest Computers that historically used (for example) "Eudora" but have been forced into using "Outlook". Arguably, this upgrade-with-change constitutes felonious unauthorized access to a Federal Interest Computer. This felony should be prosecuted aggressively.

Sincerely,

Carlie J. Coats, Jr., Ph.D. coats@emc.mcnc.org
MCNC-Environmental Modeling Center phone: (919)248-9241
North Carolina Supercomputing Center fax: (919)248-9245
3021 Cornwallis Road P. O. Box 12889
Research Triangle Park, N. C. 27709-2889 USA
"My opinions are my own, and I've got *lots* of them!"